HDE030254 EP
IB1041051363

Europäisches Patentamt | European Patent Office | Office européen des brevets

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

03102523.2

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 03102523.2 ✓
Demande no:

Anmeldetag:
Date of filing: 13.08.03 ✓
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Philips Intellectual Property & Standards
GmbH
Steindamm 94
20099 Hamburg
ALLEMAGNE
Koninklijke Philips Electronics N.V.
Groenewoudseweg 1
5621 BA Eindhoven
PAYS-BAS

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Verfahren und Vorrichtung zum Verschlüsseln eines digitalen Datenstroms in einem Übertragungssystem

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

H04B1/713

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL
PT RO SE SI SK TR LI

BESCHREIBUNG

VERFAHREN UND VORRICHTUNG ZUM VERSCHLÜSSELN EINES DIGITALEN DATENSTROMS IN EINEM ÜBERTRAGUNGSSYSTEM

Die Erfindung betrifft ein Verfahren zum Verschlüsseln eines digitalen Datenstroms in einem Übertragungssystem, welches einen Sender zum Modulieren eines digitalen Datenstroms und zum Übermitteln des modulierten digitalen Datenstroms, sowie einen Empfänger zum Empfangen des modulierten, digitalen Datenstroms und zum Zurückgewinnen des digitalen Datenstroms aufweist. Sie betrifft insbesondere ein Übertragungssystem, das auf Basis eines orthogonalen Codes die Modulation bzw. Verschlüsselung durchführt. Die Erfindung betrifft außerdem ein solches Übertragungssystem.

Die Erfindung betrifft insbesondere ein Verschlüsselungs-Verfahren, das für die Modulation einen orthogonalen Code verwendet.

Die Erfindung betrifft ferner ein Übertragungssystem, das sowohl für schnurlose, als auch für leitungsgebundene Netzwerke verwendet werden kann. Es ist anwendbar sowohl für Einträger- als auch für Mehrträgermodulation. In schnurlosen Übertragungssystemen kann sie sowohl für Systeme mit einer einzelnen Antenne, als auch für solche mit mehreren Antennen verwendet werden.

Bei einem Übertragungssystem in einem schnurlosen Netzwerk wird beispielsweise das CDMA-Verfahren (englisch: Code Division Multiple Access) verwendet. Das CDMA-Verfahren führt eine Aufteilung des Spektrums in ein breites Frequenzband durch, im folgenden Spreading genannt. Zwei Teilnehmer des Netzwerkes, die eine Verbindung aufbauen, verwenden einen bestimmten Code für die Modulation und Demodulation des Datenstromes. Der Spreading-Prozeß ist in Figur 1 zum Stand der Technik dargestellt. Der digitale Datenstrom besteht dabei aus einer sukzessiven Folge von Symbolen. Jedes Symbol des digitalen Datenstroms $d^{(k)}$ der k-ten Verbindung (link) wird während der gesamten Verbindung mit derselben Spreading-Frequenz bzw. mit

demselben Spreading-Code $c^{(k)}$ multipliziert. Der Spreading-Code $c^{(k)}$ hat die Länge P, beispielsweise 8 Bit. Diese Multiplikation ergibt das Spread-Signal $s^{(k)}$, welches durch die folgende Gleichung (1) ausgedrückt wird:

$$s^{(k)} = c^{(k)} \cdot d^{(k)} \qquad (1)$$

Der Spreading-Code $c^{(k)}$ wird dabei ausgedrückt durch folgenden Vektor (2):

$$c^{(k)} = [c_0^{(k)} \quad c_1^{(k)} \quad \ldots \quad c_{P-1}^{(k)}]^T \qquad (2)$$

Der in Gleichung (2) angegebene Vektor beschreibt einen aus positiven und negativen Rechteck-Impulsen sowie Null-Werten zusammengesetzten Spreading-Code $c^{(k)}$. Seine Periodendauer T_c beträgt konstant P Bit und drückt die Dauer der Gültigkeit eines der Elemente c_0 bis c_{P-1} aus.

Wenn wie im CDMA-Verfahren ein orthogonaler Spreading-Code verwendet wird, kann das Spread-Signal $s^{(k)}$ von dem k-ten Teilnehmer als Empfangssignal $r^{(k)}$ empfangen werden und der digitale Datenstrom zurückgewonnen werden durch Korrelation des Empfangssignals $r^{(k)}$ mit demselben Spreading-Code $c^{(k)}$, der auch beim Mischen verwendet wurde. Die Festlegung des Spreading-Codes erfolgt beispielsweise nach dem Verbindungsaufbau.

Da das CDMA-Verfahren in Netzwerken verwendet wird, in denen gleichzeitig unterschiedliche Verbindungen aufgebaut sein können, existiert eine Anzahl von unterschiedlichen Spreading-Codes. Dabei wird jeder Verbindung ein anderer Spreading-Code zugeordnet, so daß die gesendeten Daten nur bei dem berechtigten Empfänger decodiert werden können.

Die Anzahl der im CDMA-Verfahren verwendeten Spreading-Codes ist begrenzt, die Spreading-Codes selber können in Erfahrung gebracht werden. Während der gesamten Datenübertragung von einem Teilnehmer des Netzwerkes zu einem anderen wird

gemäß Gleichung (1) nur der eine, von dem sendenden Teilnehmer festgelegte Spreading-Code $c^{(k)}$ verwendet. Das führt dazu, daß von unberechtigten Empfängern abgefangene und gespeicherte Datenströme durch Korrelation des empfangenen Spektrums mit diversen orthogonalen Codes entschlüsselt werden können. Solche Systeme zur Übertragung sind also nicht abhörsicher.

Die Patentanmeldung GB 2 331 207 A offenbart ein Kommunikationssystem, das orthogonale Codes im CDMA-Verfahren verwendet. Insbesondere betrifft sie ein orthogonales Mehrfach-Zugriffssystem, welches die Kanäle entsprechend einem Hopping-Muster des orthogonalen Codes einteilt. Der Sender weist dabei einen ersten Generator für den orthogonalen Hopping-Code auf, welcher einen orthogonalen Code-Generator zum Erzeugen des orthogonalen Codes entsprechend eines Hopping-Musters und einen Hopping-Controller aufweist, welcher verbunden ist mit dem orthogonalen Code-Generator zum Erzeugen des Hopping-Musters. Bei einer Ausführungsform umfaßt der erste Generator für den Hopping-Orthogonal-Code einen Speicher zum Speichern des orthogonalen Codes für den Ausgang entsprechend dem Hopping-Muster und einen Hopping-Controller zum Erzeugen des Hopping-Musters und zum Ausgeben des Hopping-Musters an den Speicher. Dadurch, daß die orthogonalen Codes für die Verschlüsselung in einem Speicher abgelegt sind und der Zugriff auf diese orthogonalen Codes schnell erfolgen kann, wird die Geschwindigkeit der Verschlüsselung erhöht. Die Patentanmeldung GB 2 331 207 erkennt auch, daß in Verschlüsselungssystemen die Sicherheit der verschlüsselten Daten um so höher ist, je komplexer oder abwechslungsreicher die Codes für die Verschlüsselung sind. Daher schlägt die britische Patentanmeldung in einer Ausführungsform einen Sender vor, bei dem jedem Kanal ein orthogonaler Code bestehend aus Code-Symbolen zugeordnet wird, der für die Dauer der Übertragung angewandt wird. Diese orthogonalen Codes unterscheiden sich dabei bezüglich der Dauer der Gültigkeit ihrer Code-Symbole, und zwar variiert sie in bezug auf eine Daten-Einheit (Bit) des digitalen Signals. Dies bedeutet, daß die einzelnen Elemente $c_0^{(k)}$, $c_1^{(k)}$ ... $c_{P-1}^{(k)}$ der P Elemente eines Vektors aus Gleichung (2) dieselbe Gültigkeitsdauer haben, diese Gültigkeitsdauer jedoch unterschiedlich ist zu der der Elemente einer anderen Verbindung. Anders herum

ausgedrückt weisen unterschiedliche orthogonale Codes unterschiedliche Sprung-Zeiten T_{hop} (hopping period) auf. Durch die Verwendung von unterschiedlichen orthogonalen Codes, die sich bezüglich der Sprung-Zeit T_{hop} unterscheiden, für unterschiedliche Kanäle wird senderseitig eine Verschlüsselungs-Funktion bzw. empfängerseitig eine Entschlüsselungs-Funktion realisiert, die aber nur auf das gesamte Kommunikationssystem abzielt und nicht auf die einzelnen Kanäle, von denen jeder einen konstant anzuwendenden Spreading-Code zugeteilt bekommt. Die orthogonalen Codes werden von einem Hopping Code Generator (HCG) gemäß einem vom Hopping Controller auswählbaren Hopping-Muster erzeugt. Die Sprungzeit eines einzelnen orthogonalen Codes kann dabei kürzer sein als die Dauer einer Dateneinheit, identisch sein mit der Dauer einer Dateneinheit, oder das n-fache der Länge einer Dateneinheit betragen, wobei n eine ganze Zahl ist.

Die internationale Patentanmeldung WO 02/056517 A1 offenbart ein Verfahren zum Betreiben eines CDMA-Kommunikationssystems, das in einem Versorgungsbereich einer Basisstation eine Spreading-Codes aus einer Menge von Spreading-Codes einzelnen Teilnehmern einer Vielzahl von Teilnehmerstationen zuweist und das dann während der Übertragung innerhalb der Zelle periodisch zwischen den Spreading-Codes hüpft, und zwar innerhalb der Menge von Spreading-Codes. Damit zu jeder beliebigen Zeit keine zwei Teilnehmerstationen mit demselben Spreading-Code arbeiten, werden alle Teilnehmer zueinander versetzt in einer Tabelle registriert, welche die PN Codes beinhaltet. Innerhalb der Tabelle werden die Teilnehmer in gleichem Maße bewegt, so daß sie unter Beibehaltung ihres Versatzes von einem Code zu einem anderen hüpfen. Somit arbeitet jeder Teilnehmer innerhalb der Zelle für einen vorbestimmten Zeitabschnitt mit einem unterschiedlichen PN Spreading-Code. Der Schritt des periodischen Hüpfens wechselt bevorzugt von dem aktuell verwendeten Spreading-Code zu dem nächsten Spreading-Code mit einer Symbolrate oder einem Vielfachen der Symbolrate. Das System kann eines mit einer festen Datenrate oder mit einer variablen Datenrate sein. Entscheidend ist dabei, daß alle in der Tabelle registrierten Teilnehmer in gleichem Maße bewegt werden, damit ihr Versatz beibehalten wird und somit sichergestellt wird, daß jeder Teilnehmer mit einem anderen

Spreading-Code arbeitet. Um dies sicherzustellen, erfolgt die Zuweisung der Spreading-Codes und des Musters für das Hüpfen zentralisiert und abgestimmt. Das Muster für das Hüpfen ist festgelegt und eben jedem Teilnehmer bekannt, damit sichergestellt ist, daß der Abstand der Teilnehmer in der Tabelle beibehalten wird. Durch das Hüpfen von dem aktuell verwendete Spreading-Code zu einem anderen Spreading-Code wird die eventuell vorhandene Störung zwischen zwei Teilnehmern reduziert.

Aufgabe der Erfindung ist es, ein Verfahren zum Verschlüsseln eines digitalen Datenstroms in einem Übertragungssystem, das für die Modulation orthogonale Codes verwendet, anzugeben, das die Abhörsicherheit des Datenstroms erhöht. Des weiteren ist es Aufgabe der Erfindung, ein Verfahren zum Entschlüsseln eines verschlüsselt gesendeten digitalen Datenstroms anzugeben. Es ist ferner Aufgabe der Erfindung, eine Vorrichtung zum Durchführen eines solchen Verfahrens anzugeben. Es ist außerdem Aufgabe der Erfindung, ein solches Übertragungssystem für einen digitalen Datenstrom anzugeben, das für die Modulation orthogonale Codes verwendet und eine erhöhte Abhörsicherheit aufweist.

Das Erhöhen des Verschlüsselungsgrades durch Variieren der Verschlüsselung wie in Patentanspruch 1 beschrieben während einer bestehenden Verbindung erschwert es einem unberechtigten Dritten, auf Basis von abgefangenen Daten durch Ausprobieren sämtlicher bekannter Spreading-Codes den Inhalt des Datenstroms zu ermitteln, da jeder einzelne, wenn auch an sich bekannte Spreading-Code, nur für eine kurze Zeit angewandt wird, und dann in einer quasi zufälligen Reihenfolge ein anderer Spreading-Code aus der festgelegten Menge angewandt wird und/oder die Länge des Sprung-Intervalls von einem zum nächsten Spreading-Code variiert wird.

Die zugewiesene Reihenfolge für die Anwendung der unterschiedlichen Spreading-Codes ist nur für eine einzelne k-te Verbindung gültig und nur der sendenden und der empfangenden Vorrichtung bekannt. Diese Reihenfolge wird nicht zentral erzeugt und ist nicht mehreren Verbindungen zugeordnet, so daß die zugewiesene Reihenfolge einer

bestimmten Verbindung anderen nicht bekannt ist. Die Reihenfolge wird dabei von der sendenden Vorrichtung festgelegt und ist beispielsweise von einem Zufallsgenerator erzeugt oder einer in einem Speicher abgelegten Tabelle entnommen. Die Reihenfolge für die Anwendung der unterschiedlichen Spreading-Codes hat dabei bevorzugt zufälligen Charakter.

Das einer k-ten Verbindung zugewiesene Sprung-Intervall gibt die Gültigkeit für einen Spreading-Code an und kann als Periodendauer, also einer zeitlichen Gültigkeitsdauer oder als eine Anzahl von Datenpaketen definiert sein. Das Sprung-Intervall wird dezentral von der sendenden Vorrichtung festgelegt und der empfangenden Vorrichtung mitgeteilt. Dies bedeutet, daß in einem Netzwerk, in dem mehrere Verbindungen gleichzeitig bestehen, wobei diese Verbindungen jeweils einen Satz von Spreading-Codes verwenden, diese inhaltlich Überschneidungen haben können derart, daß einzelne Verbindungen zeitweise durchaus identische Spreading-Codes verwendet werden könnten, diese jedoch nur vorübergehend zeitgleich verwendet werden, da nach Ablauf des Sprung-Intervalls ein anderer Spreading-Code verwendet wird.

Die Reihenfolge der Anwendung des Inhaltes eines Satzes von Spreading-Codes kann durch eine Permutations-Funktion definiert werden, die als Vektor aufgebaut ist und die jeweilige Position des aktuell zu verwendenden Spreading-Codes angibt. Dabei steht an erster Stelle des Vektors die Position des ersten anzuwendenden Spreading-Codes, an zweiter Stelle die Position des zweiten anzuwendenden Spreading-Codes usw. Insgesamt beinhaltet die Permutations-Funktion M Elemente. Ist der Vektor einmal durchlaufen, wird die Zuweisung wieder im Sinne einer Schleife an der ersten Position begonnen. Die Angabe der Positionen des Spreading-Codes erfolgt bevorzugt durch ganze Zahlen.

Bei dem in Patentanspruch 3 beschriebenen Verfahren werden nach dem Verbindungsaufbau die für die Übermittlung und Wiederherstellung des digitalen Datenstroms erforderlichen Parameter mittels eines Encryption Keys übertragen. Durch das Übermitteln des Encryption Keys werden folgende Schritte veranlaßt:

- Festlegen einer Permutations-Funktion,
- Festlegen eines Satzes von Spreading-Codes, und/oder
- Festlegen eines Sprung-Intervalls,

wobei einer, zwei oder alle drei letztgenannte Schritte durchgeführt werden können, und zwar in beliebiger Reihenfolge, da die Übermittlung des Encryption Keys abgeschlossen ist, bevor die Übertragung des digitalen Datenstroms beginnt.

Bei dem im Patentanspruch 4 beschriebenen Verfahren zum Verschlüsseln eines digitalen Datenstroms wird ein erster Permutations-Ablauf durchgeführt, welcher eine Schleife mit folgenden Schritten beinhaltet:

- Setzen eines Intervalls auf "1";
- Abwarten des Endes eines vordefinierten Sprung-Intervalls;
- Erhöhen des Intervalls um den Wert 1;
- Durchführen eines Vergleichs, ob der aktuelle Wert des Intervalls größer ist, als die gesamte Anzahl der Elemente einer Permutations-Funktion, welche die Positionen des für das Verschlüsseln des digitalen Datenstroms zu verwendenden Spreading-Codes eines Satzes von Spreading-Codes angibt, wobei alternativ erfolgt
  - -- wenn der Vergleich positiv ausgeht: Zurücksetzen des Intervalls auf "1";
  - -- wenn der Vergleich negativ ausgeht: Gleichsetzen des augenblicklichen Spreading-Code mit dem Spreading-Code, der an der von der Permutations-Funktion vorgegebenen Position steht.

Diese Verfahren beschreibt das Definieren bzw. Zuweisen des jeweils augenblicklich zu verwendenden Spreading-Codes.

Bezüglich der Vorrichtung zum Durchführen eines Verschlüsselungs-Verfahrens wird die Aufgabe erfindungsgemäß dadurch gelöst, daß die Vorrichtung einen ersten Code-Generator aufweist, der den jeweils aktuellen Spreading-Code erzeugt. Die Erzeugung des jeweils aktuellen Spreading-Codes kann dabei zeitgleich während der Verschlüsselung erfolgen oder vor der Verschlüsselung abgeschlossen sein, wobei dann die während der Verschlüsselung anzuwendenden Spreading-Codes beispielsweise in einer Tabelle in einem ROM oder sonstigem Speicher abgelegt sind.

Bezüglich des Verfahrens zum Entschlüsseln eines empfangenen, verschlüsselt gesendeten digitalen Datenstroms wird die Aufgabe erfindungsgemäß gelöst durch das Durchführen eines zweiten Permutations-Ablaufs, der eine Schleife mit folgenden Schritten beinhaltet:

- Setzen eines Intervalls auf "1";
- Abwarten des Endes eines vordefinierten Sprung-Intervalls;
- Erhöhen des Intervalls um den Wert 1;
- Durchführen eines Vergleichs, ob der aktuelle Wert des Intervalls größter ist, als die gesamte Anzahl der Elemente einer Permutations-Funktion, welche die Positionen der für das Entschlüsseln des verschlüsselten digitalen Datenstroms zu verwendenden Spreading-Codes eines Satzes von Spreading-Codes angibt, wobei alternativ erfolgt:
  - -- wenn der Vergleich positiv ausgeht: Zurücksetzen des Intervalls auf "1";
  - -- wenn der Vergleich negativ ausgeht: Gleichsetzen des augenblicklichen Spreading-Codes mit dem Spreading-Code, der an der von der Permutations-Funktion vorgegebenen Position steht.

Die hier beschriebene Schleife sorgt dafür, daß das empfangene Signal jeweils mit demselben Code entschlüsselt wird, der für die Verschlüsselung verwendet wurde, und dadurch der digitale Datenstrom wiederhergestellt wird.

Bezüglich der Vorrichtung zum Ausführen eines Entschlüsselungs-Verfahrens ist die Aufgabe erfindungsgemäß dadurch gelöst, daß die Vorrichtung einen zweiten Code-Generator aufweist, der den aktuellen Spreading-Code erzeugt. Der aktuelle Spreading-Code kann dabei zeitgleich während der Entschlüsselung erzeugt werden oder vorab erzeugt sein und in einem geeigneten Speicher hinterlegt sein. Ein zweiter Code-Generator meint in diesem Fall, daß sowohl die sendende Vorrichtung, als auch die empfangende Vorrichtung einen Code-Generator aufweisen. Der während der k-ten Verbindung als zweiter Code-Generator, nämlich als Code-Generator für die Entschlüsselung, eingesetzte Code-Generator, kann während einer anderen Verbindung,

bei der diese Vorrichtung sendet, auch der für die Verschlüsselung verwendete erste Code-Generator sein.

Bezüglich des Übertragungssystems für einen digitalen Datenstrom, das für die Modulation orthogonale Codes verwendet, wird die Aufgabe erfindungsgemäß dadurch gelöst, daß das Übertragungssystem eine erste Vorrichtung aufweist, in der der digitale Datenstrom mit einem Spreading-Code gemischt wird und eine zweite Vorrichtung aufweist, in der das empfangene, verschlüsselte Signal und der Spreading-Code einem Korrelator zugeführt werden und das Übertragungssystem Mittel aufweist zum

- Durchführen einer Verschlüsselung,
- Durchführen einer Entschlüsselung eines verschlüsselt gesendeten, digitalen Datenstroms.

Diese Mittel können sein ein Taktgenerator, ein Speicher (ROM) für die Ablage des Spreading-Codes und der Zuweisungen, die mit Hilfe des Encryption Keys übermittelt werden, abgelegt werden.

Die erfindungsgemäßen Verfahren zum Verschlüsseln und Entschlüsseln eines digitalen Datenstroms können sowohl in schnurlosen als auch in leitungsgebundenen Netzwerken verwendet werden, wobei die Höhe des Verschlüsselungsgrades und somit die Höhe des Schutzes vor unberechtigtem Abhören an die jeweilige Anforderung angepaßt werden kann.

Vorteile der Erfindung sind, daß der Verschlüsselungsgrad bei der Datenübertragung erhöht wird, dabei aber die erforderliche Bandbreite unverändert bleibt. Dieser Vorteil wird dadurch erreicht, daß die Verschlüsselung der digitalisierten Daten in der physikalischen Schicht (Layer 1) des OSI 7-Schichten-Modell stattfindet.

Verschlüsselungsgrad besteht in diesem Zusammenhang für einen Pegel von Komplexität. Die Maßnahmen

1) Verwenden eines Satzes unterschiedlicher Spreading-Codes,
2) Verwenden einer Permutations-Funktion und/oder

3) Verwenden eines Sprung-Intervalls, das für unterschiedliche Verbindungen unterschiedlich lang ist,

können einzeln oder in Verbindung angewandt werden. Je mehr Maßnahmen realisiert werden, desto höher ist der Pegel der Komplexität und somit der Verschlüsselungsgrad. Die Komplexität wird weiterhin erhöht durch Verwenden von Faktoren größeren Inhalts und somit durch größere Abwechslung.

Die Erfindung wird im folgenden lediglich beispielhaft erläutert, wobei

Figur 1 zum Stand der Technik schematisch einen CDMA-Sender zeigt;

Figur 2 zum Stand der Technik schematisch einen CDMA-Empfänger zeigt;

Figur 3 in einer schematischen Darstellung eine erfindungsgemäße Vorrichtung zum Verschlüsseln zeigt;

Figur 4 in einer schematischen eine erfindungsgemäße Vorrichtung zum Entschlüsseln zeigt;

Figur 5 in einer schematischen Darstellung einem Ablaufdiagramm schematisch ein erfindungsgemäßes Verfahren zum Verschlüsseln eines digitalen Datenstroms darstellt;

Figur 6 in einem Ablaufdiagramm schematisch ein erfindungsgemäßes Verfahren zum Entschlüsseln und Wiederherstellen eines digitalen Datenstroms darstellt und

Figur 7 eine Tabelle mit bestimmten Permutations-Funktionen beinhaltet.

Figur 1 zeigt zum Stand der Technik schematisch einen Sender für die Übertragung mit dem CDMA-Verfahren. Der digitale Datenstrom $d^{(k)}$ der k-ten Verbindung wird mit einem Spreading-Code $c^{(k)}$ gemischt. Das so erzeugte Sende-Signal $s^{(k)}$ wird schnurlos oder leitungsgebunden an den empfangenen Teilnehmer geschickt. Der Spreading-Code $c^{(k)}$ ist für die Dauer der Verbindung konstant. Ein unberechtigter Empfänger kann das Sende-Signal $s^{(k)}$ abfangen und speichern und könnte durch Ausprobieren den einzigen verwendeten Spreading-Code ermitteln.

Figur 2 zeigt zum Stand der Technik schematisch einen CDMA-Empfänger, der das

codierte Eingangssignal $r^{(k)}$ in einem Korrelator demselben Spreading-Code $c^{(k)}$ hinzufügt. Der eine Spreading-Code $c^{(k)}$ wird dem Empfänger für die k-te Verbindung mitgeteilt. Wenn bei der Korrelation der Spreading-Code $c^{(k)}$ verwendet wird, der auch beim Codieren angewandt wurde, kann das empfangene Signal $r^{(k)}$ decodiert werden und somit der digitale zum Datenstrom $y^{(k)}$ wieder hergestellt werden.

Figur 3 zeigt in einer schematischen Darstellung eine erfindungsgemäße Vorrichtung 1 zum Verschlüsseln für das CDMA-Übertragungssystem. Der digitale Datenstrom $d^{(k)}$ wird hierbei mit einem dynamischen Code $c^{(k)}(t)$ gemischt. Ein dynamischer Code-Generator 2 erzeugt orthogonale Codes unterschiedlichen Inhaltes und steuert deren Anwendung, so daß während einer Verbindung unterschiedliche Spreading-Codes angewandt werden. Mit einem nach dem Verbindungsaufbau übermittelten Encryption Key wird unter anderem eine Menge G_i von orthogonalen Codes $\{g_1^{(k)}, g_2^{(k)} \ldots g_H^{(k)}\}$ festgelegt. Während einer Verbindung werden nacheinander wenigstens zwei Codes aus der Menge G_i verwendet. Die Kennzeichnung des dynamischen Spreading-Codes $c^{(k)}(t)$ soll bedeuten, daß während der Verbindung die Verschlüsselung variiert, beispielsweise durch Anwenden eines ersten Code $c_1^{(k)}$, eines zweiten Codes $c_2^{(k)}$ usw. Je nach Dauer der Verbindung oder Definition des Sprungintervalls I_{hop} eines Spreading-Codes können einzelne oder alle Codes mehrfach verwendet werden. Durch Wechseln des Spreading-Codes während der Übertragung wird ein erster Verschlüsselungs-Grad erreicht.

Figur 4 zeigt in einer schematischen Darstellung eine erfindungsgemäße Vorrichtung 3 zum Entschlüsseln des empfangenen Signals $r^{(k)}$ und zum Wiederherstellen des digitalen Datenstroms $y^{(k)}$ in einem Übertragungssystem. Das empfangene Signal $r^{(k)}$ wird hierbei ebenso wie der dynamische Code $c^{(k)}(t)$ einem Korrelator zugeführt. Ein dynamischer, zweiter Code-Generator 4 erzeugt dabei orthogonale Codes unterschiedlichen Inhalts und steuert deren Anwendung, so daß während einer Verbindung unterschiedliche Spreading-Codes angewandt werden. Das Anwenden unterschiedlicher Spreading-Codes während einer einzelnen Verbindung soll durch die Darstellung (t) und durch das Adjektiv "dynamisch" visualisiert werden.

Der dynamische Code-Generator 2 für die Sendevorrichtung 1 und der Code-Generator 4 für die Empfangsvorrichtung können physikalisch dieselben sein. Beispielsweise hat ein Mobilfunk-Telefon einen Part zum Senden und einen Part zum Empfangen, wobei beide nach einer Ausführungsform der Erfindung auf denselben dynamischen Code-Generator zugreifen.

Figur 5 stellt in einem Ablaufdiagramm schematisch ein erfindungsgemäßes Verfahren zum Verschlüsseln eines digitalen Datenstroms dar. Im Anschluß an den Verbindungsaufbau 100 wird in Schritt 200 der Encryption Key übermittelt. Dieser veranlaßt in beliebiger Reihenfolge folgendes:

- das Festlegen einer Permutations-Funktion S_i 210;
- das Festlegen eines Satzes Spreading-Codes G_i 220;
- das Festlegen eines Sprung-Intervalls I_{hop} 230.

Der Encryption Key wird von der sendenden Einheit erzeugt und beinhaltet die für Entschlüsselung des übertragenen Datensignals erforderlichen Parameter.

Die Permutations-Funktion $S_i = \{p\_1, p\_2 \ldots p\_M\}$ gibt an, in welcher Reihenfolge die einzelnen Codes $g_1^{(k)}, g_2^{(k)} \ldots g_H^{(k)}$ des Satzes G_i angewandt werden. Das Festlegen 210 der für die aktuelle Übertragung gültigen Permutations-Funktion kann alternativ erfolgen durch:

a) Übermitteln eines Vektors S_i, der die konkrete Permutations-Folge {p_1, p_2 ... p_M} beinhaltet, oder
b) Übermitteln nur des Namens einer einzelnen Permutations-Funktion S_i.

Die Alternative a) ermöglicht einem unberechtigten dritten Teilnehmer die Permutations-Folge abzuhören und somit ein Hilfsmittel zum Entschlüsseln des gesendeten digitalen Datenstroms zu erhalten. Dieses Verfahren hat aber den Vorteil, daß sowohl senderseitig, als auch empfängerseitig Speicherplatz gespart wird, da die für die aktuelle Übermittlung gültige Permutations-Folge nur zwischengespeichert zu

werden braucht und nach Beendigung der Übertragung gelöscht werden kann.

Die Alternative b) setzt voraus, daß sowohl senderseitig, als auch empfängerseitig alle möglichen Permutations-Funktionen S_1, S_2 ... S_L (L: ganzzahlig) dauerhaft gespeichert sein müssen, damit die für die Übertragung gültige Permutations-Funktion S_i aufgerufen werden kann. Vorteil dieser Variante ist, daß ein unberechtiger dritter Teilnehmer die hinter der verwendeten Permutations-Funktion S_i steckende Folge von orthogonalen Codes G_i nicht ermitteln kann, da sie nicht übermittelt wird, wobei H und P ganzzahlig sind.

Ein Satz G_i beinhaltet H einzelne orthogonale Codes, die geeignet sind, im CDMA-Verfahren angewandt zu werden. Jeder einzelne der H orthogonalen Codes g ist dabei als Vektor mit P Elementen aufgebaut.

Der Schritt des Festlegens eines Satzes G_i von Spreading-Codes 220 kann alternativ erfolgen durch
entweder
c) Übermitteln der konkreten, einzelnen orthogonalen Codes in Form von Vektoren
oder
d) Übermittlung der Namen der anzuwendenden orthogonalen Codes.

Die Vor- und Nachteile der Alternativen c) und d) sind wie bei den Alternativen a) und b) beim Festlegen der Permutations-Funktion S_i die, daß das Übermitteln der konkreten Angaben die Abhörsicherheit verringert, daß das Speichern und Aufrufen vordefinierter orthogonaler Codes sowohl sender-, als auch empfängerseitig Speicherplatz beansprucht.

Der Schritt 230 des Festlegens des Sprung-Intervalls I_{hop} bedeutet alternativ
entweder
e) Vorgabe einer Periodendauer T_{hop}, also einer zeitlichen Gültigkeitsdauer,
oder

f) Vorgabe einer Anzahl Q von Datenpaketen.

Nach Übermitteln des Encryption Keys beginnt das dynamische Verschlüsseln 300. Der erste Permutations-Ablauf 400 ist der folgende: bei Schritt 410 wird das Intervall n auf "1" gesetzt, derjenige orthogonale Code aus dem Satz G_i verwendet, der an der Stelle p_1 der Permutations-Funktion S_i steht. Bei Schritt 420 wird der Ablauf des Sprung-Intervalls I_{hop} abgewartet. Das Messen der Zeit zum Ermitteln des Endes der Periodendauer bzw. das Zählen der übermittelten Datenpakete erfolgt durch entsprechende Vorrichtungen, wie zum Beispiel einen Zähler oder ein Flip-Flop. Wenn das Ende des Sprungintervalls I_{hop} erreicht ist, wird in Schritt 430 das Intervall n um den Wert 1 erhöht. Bei Schritt 440 wird dann der Vergleich durchgeführt, ob der aktuelle Wert für das Intervall n größer ist, als die gesamte Anzahl M der Elemente des Permutations-Vektors. Ergibt der Vergleich "Ja", beginnt die Schleife wieder mit Schritt 410 und wird das Intervall n wieder auf "1" gesetzt. Ist das Ergebnis des Vergleichs "Nein", wird in Schritt 450 als augenblicklicher Code $c_n^{(k)}$ derjenige aufgerufen, der an der n-ten Position p_n der Permutations-Funktion S_i steht, also $c_n^{(k)} = g_{p\_n}^{(k)}$ und solange angewandt, bis im Zuge der Schleife in Schritt 420 das Ende des Sprung-Intervalls I_{hop} erreicht ist und anschließend in Schritt 430 das Intervall n um den Wert 1 erhöht wird.

Figur 6 stellt in einem Ablaufdiagramm schematisch ein erfindungsgemäße Verfahren zum Entschlüsseln und Wiederherstellen eines digitalen Datenstroms dar. Der im Anschluß an den Verbindungsaufbau 500 in Schritt 600 übermittelte Encryption Key veranlaßt folgendes:

- das Festlegen einer Permutations-Funktion S_i 610;
- das Festlegen eines Satzes Spreading-Codes G_i 620;
- das Festlegen eines Sprung-Intervalls I_{hop} 630.

Wie bereits zu Fig. 5 erläutert kann

- das Festlegen 610 der für die aktuelle Übertragung gültigen Permutations-Funktion alternativ erfolgen durch entweder Übermitteln eines Vektors S_i, der die konkrete

Permutations-Folge {p_1, p_2 ... p_M} beinhaltet, oder Übermitteln nur des Namens einer einzelnen Permutations-Funktion S_i,

- der Schritt des Festlegens eines Satzes G_i von Spreading-Codes 620 alternativ erfolgen durch entweder Übermitteln der konkreten, einzelnen orthogonalen Codes in Form von Vektoren oder Übermittlung der Namen der anzuwendenden orthogonalen Codes und/oder
- der Schritt 630 des Festlegens des Sprung-Intervalls I_{hop} alternativ eine Vorgabe entweder einer Periodendauer T_{hop}, also einer zeitlichen Gültigkeitsdauer, oder einer Anzahl Q von Datenpaketen bedeuten.

Nach Übermitteln des Encryption Keys beginnt das dynamische Entschlüsseln 700. Der erste Permutations-Ablauf 800 ist der folgende: bei Schritt 810 wird das Intervall n auf "1" gesetzt, derjenige orthogonale Code aus dem Satz G_i verwendet, der an der Stelle p_1 der Permutations-Funktion S_i steht. Bei Schritt 820 wird der Ablauf des Sprung-Intervalls I_{hop} abgewartet. Das Messen der Zeit zum Ermitteln des Endes der Periodendauer bzw. das Zählen der übermittelten Datenpakete erfolgt durch entsprechende Vorrichtungen, wie zum Beispiel einen Zähler oder ein Flip-Flop. Wenn das Ende des Sprungintervalls I_{hop} erreicht ist, wird in Schritt 830 das Intervall n um den Wert 1 erhöht. Bei Schritt 840 wird dann der Vergleich durchgeführt, ob der aktuelle Wert für das Intervall n größer ist, als die gesamte Anzahl M der Elemente des Permutations-Vektors. Ergibt der Vergleich "Ja", beginnt die Schleife wieder mit Schritt 810 und wird das Intervall n wieder auf "1" gesetzt. Ist das Ergebnis des Vergleichs "Nein", wird in Schritt 850 als augenblicklicher Code $c_n^{(k)}$ derjenige aufgerufen, der an der n-ten Position p_n der Permutations-Funktion S_i steht, also $c_n^{(k)} = g_{p\_n}^{(k)}$ und solange angewandt, bis im Zuge der Schleife in Schritt 820 das Ende des Sprung-Intervalls I_{hop} erreicht ist und anschließend in Schritt 830 das Intervall n um den Wert 1 erhöht wird.

Figur 7 beinhaltet eine Tabelle mit Beispielen für bestimmte Permutations-Funktionen $S_i = \{p\_1, p\_2 \ldots p\_M\}$ und dem daraus folgenden Code c_i. Dabei sind p_1, p_2 ... p_M beliebige ganze Zahlen 1, 2 ... H. Wenn eine bestimmte Permutations-Funktion

beispielsweise lautet: $s = \{2, H\}$, bedeutet dies, daß $p\_1 = 2$ und $p\_2 = H$ ist und beim Verschlüsseln zunächst der Spreading-Code g_2 und anschließend der Spreading-Code g_H angewandt wird. Sollte die Verbindung dann noch nicht beendet sein, wird das Verschlüsseln im Sinne einer Schleife fortgesetzt mit p_1, also g_2, und dann mit p_2, also g_H.

PATENTANSPRÜCHE

1. Verfahren zum Verschüsseln eines digitalen Datenstroms in einem Übertragungssystem, das für die Modulation orthogonale Codes verwendet, wobei
- ein k-ter Sender eine k-te Verbindung für den k-ten digitalen Datenstrom ($d^{(k)}$) aufbaut,
- für das Verschüsseln der digitale Datenstrom ($d^{(k)}$) des Senders mit einem dieser k-ten Verbindung zugewiesenen Spreading-Code gemischt wird,
- unterschiedliche Spreading-Codes ($g_1^{(k)}$, $g_2^{(k)}$ ... $g_H^{(k)}$) aus einem definierten Satz (G_i) zugewiesen werden und
- durch das Mischen ein Sende-Signal ($s^{(k)}$) erzeugt wird,
dadurch gekennzeichnet,
daß der Verschlüsselungsgrad des k-ten digitalen Datenstrom ($d^{(k)}$) während der k-ten Verbindung erhöht wird durch Zuweisen
• einer Reihenfolge für die Anwendung der unterschiedlichen Spreading-Codes ($g_1^{(k)}$, $g_2^{(k)}$ ... $g_H^{(k)}$) und/oder
• eines Sprung-Intervalls (I_{hop}).

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet,
daß eine Permutations-Funktion (S_i) die Reihenfolge der Anwendung des Inhalts eines Satzes von Spreading-Codes (G_i) durch Angabe der Position ({p_1, p_2 ... p_M}) definiert.

3. Verfahren zum Verschlüsseln eines zu sendenden digitalen Datenstroms, wobei nach dem Verbindungsaufbau für die Übermittlung und Wiederherstellung erforderliche Parameter übertragen werden, gekennzeichnet durch die Schritte:
   - Übermitteln eines Encryption Keys (200) und dadurch:
     -- Festlegen (210) einer Permutations-Funktion (S_i),
     -- Festlegen (220) eines Satzes (G_i) von Spreading-Codes, und/oder
     -- Festlegen (230) eines Sprung-Intervalls (I_{hop}),

   wobei die letztgenannten drei Schritte (210, 220, 230) in beliebiger Reihenfolge durchgeführt werden können.

4. Verfahren zum Verschlüsseln eines digitalen Datenstroms, gekennzeichnet durch das Durchführen eines ersten Permutations-Ablaufs (400), der eine Schleife mit folgenden Schritten beinhaltet:
   - Setzen (410) eines Intervalls (n) auf "1";
   - Abwarten (420) des Endes eines vordefinierten Sprung-Intervalls (I_{hop});
   - Erhöhen (430) des Intervalls (n) um den Wert 1;
   - Durchführen eines Vergleichs (440), ob der aktuelle Wert des Intervalls (n) größer ist, als die gesamte Anzahl (M) der Elemente einer Permutations-Funktion (S_i), welche die Positionen des für das Verschlüsseln des digitalen Datenstroms zu verwendenden Spreading-Codes (g_n) eines Satzes (G_i) von Spreading-Codes angibt, wobei alternativ erfolgt
     -- wenn der Vergleich positiv ausgeht: Zurücksetzen des Intervalls (n) auf "1";
     -- wenn der Vergleich negativ ausgeht: Gleichsetzen des augenblicklichen Spreading-Codes (g_n) mit dem Spreading-Code (g_{p_n}), der an der von der Permutations-Funktion (S_i) vorgegebenen Position (p_n) steht.

5. Vorrichtung (1) zum Ausführen eines Verfahrens nach einem der vorangehenden Ansprüche,
dadurch gekennzeichnet,
daß die Vorrichtung einen ersten Code-Generator (2) aufweist, der den jeweils aktuellen Spreading-Code (g_n) erzeugt.

6. Verfahren zum Entschlüsseln eines empfangenen, verschlüsselt gesendeten digitalen Datenstroms, gekennzeichnet, durch das Durchführen eines zweiten Permutations-Ablaufs (800), der eine Schleife mit folgenden Schritten beinhaltet:
- Setzen (810) eines Intervalls (n) auf "1";
- Abwarten (820) des Endes eines vordefinierten Sprung-Intervalls (I_{hop});
- Erhöhen (830) des Intervalls (n) um den Wert 1;
- Durchführen eines Vergleichs (840), ob der aktuelle Wert des Intervalls (n) größer ist, als die gesamte Anzahl (M) der Elemente einer Permutations-Funktion (S_i), welche die Positionen der für das Entschlüsseln des verschlüsselten digitalen Datenstroms zu verwendenden Spreading-Codes (g_n) eines Satzes (G_i) von Spreading-Codes angibt, wobei alternativ erfolgt,
  -- wenn der Vergleich positiv ausgeht: Zurücksetzen des Intervalls (n) auf "1";
  -- wenn der Vergleich negativ ausgeht: Gleichsetzen des augenblicklichen Spreading-Codes (g_n) mit dem Spreading-Code (g_{p_n}), der an der von der Permutations-Funktion (S_i) vorgegebenen Position (p_n) steht.

7. Vorrichtung (3) zum Ausführen eines Verfahrens nach Anspruch 6,
dadurch gekennzeichnet,
daß die Vorrichtung (3) einen zweiten Code-Generator (4) aufweist, der den aktuellen Spreading-Code (g_n) erzeugt.

8. Übertragungssystem, das für die Modulation orthogonale Codes verwendet, mit einer Vorrichtung zum Verschlüsseln eines digitalen Datenstroms, insbesondere eine Vorrichtung (1) nach Anspruch 5, wobei der digitale Datenstrom ($d^{(k)}$) mit einem Spreading-Code gemischt wird, und mit einer Vorrichtung zum Entschlüsseln eines verschlüsselt gesendete, digitalen Datenstroms, insbesondere eine Vorrichtung (3) nach Anspruch 6,
dadurch gekennzeichnet,
daß es Mittel aufweist zum
   - Durchführen einer Verschlüsselung,
   - Durchführen einer Entschlüsselung eines verschlüsselt gesendeten, digitalen Datenstroms.

9. Verwendung eines der vorgenannten Verfahren in einem schnurlosen oder in einem leitungsgebundenen Netzwerk.

ZUSAMMENFASSUNG

VERFAHREN UND VORRICHTUNG ZUM VERSCHLÜSSELN EINES DIGITALEN DATENSTROMS IN EINEM ÜBERTRAGUNGSSYSTEM

Verfahren zum Verschlüsseln eines digitalen Datenstroms ($d^{(k)}$) mittels eines dynamischen orthogonalen Spreading-Codes ($g_1^{(k)}$, $g_2^{(k)}$ ... $g_H^{(k)}$) und durch Zuweisen eines Sprung-Intervalls (I_{hop}), welches von Verbindung zu Verbindung variiert. Der Verschlüsselungsgrad wird weiterhin erhöht durch Variieren der Reihenfolge der Anwendung des Inhaltes eines Satzes (G_i) von Spreading-Codes, die durch Angabe der Positionen ({p_1, p_2 ... p_M}) in einer Permutations-Funktion (S_i) definiert ist.

(Figur 3)

Fig. 1
Stand der Technik

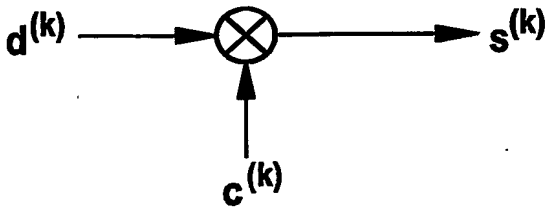

Fig. 2
Stand der Technik

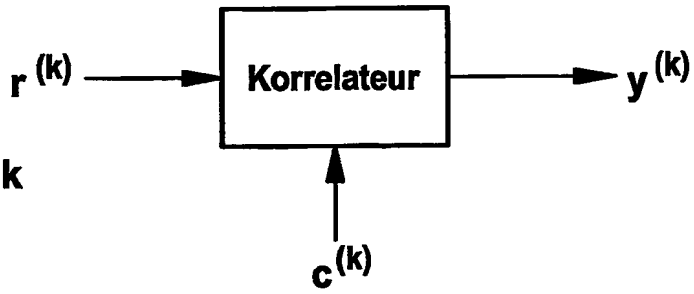

Fig. 3

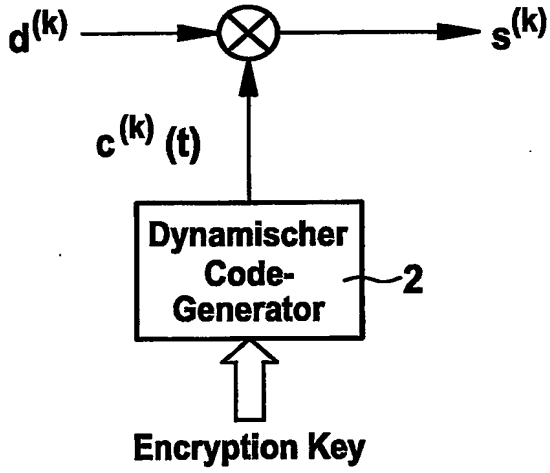

Fig. 4

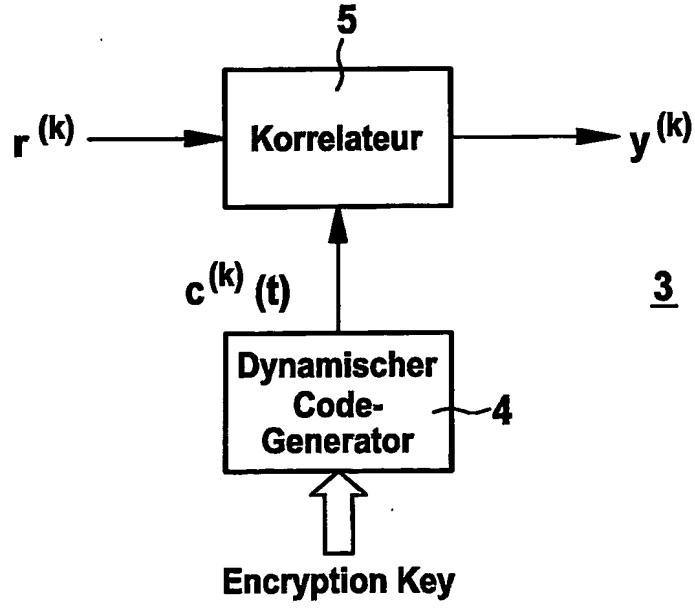

Fig. 5

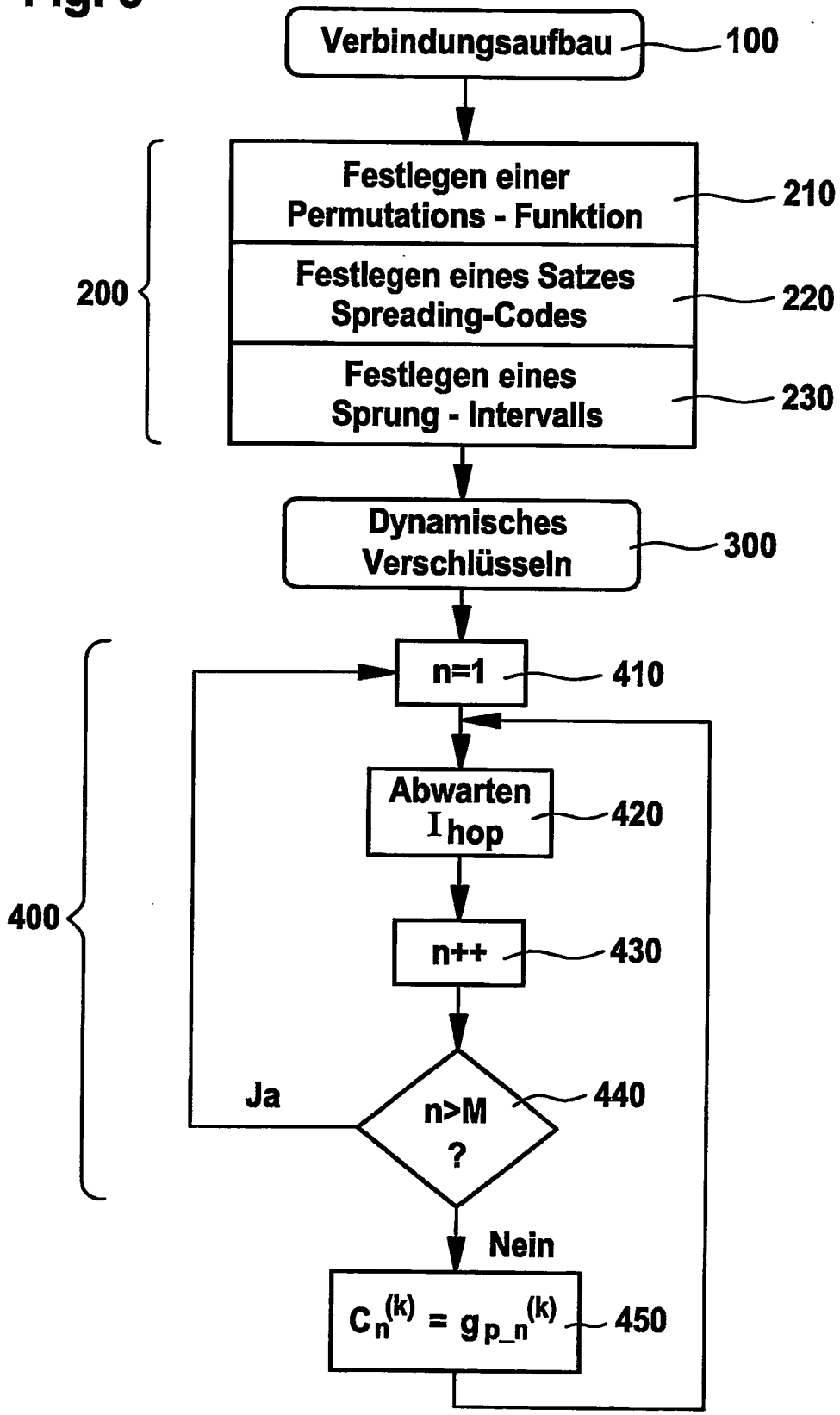
Verbindungsaufbau
100
200
Festlegen einer Permutations - Funktion
210
Festlegen eines Satzes Spreading-Codes
220
Festlegen eines Sprung - Intervalls
230
Dynamisches Verschlüsseln
300
400
n=1
410
Abwarten I_{hop}
420
n++
430
Ja
n>M ?
440
Nein
$C_n^{(k)} = g_{p\_n}^{(k)}$
450

Fig. 6

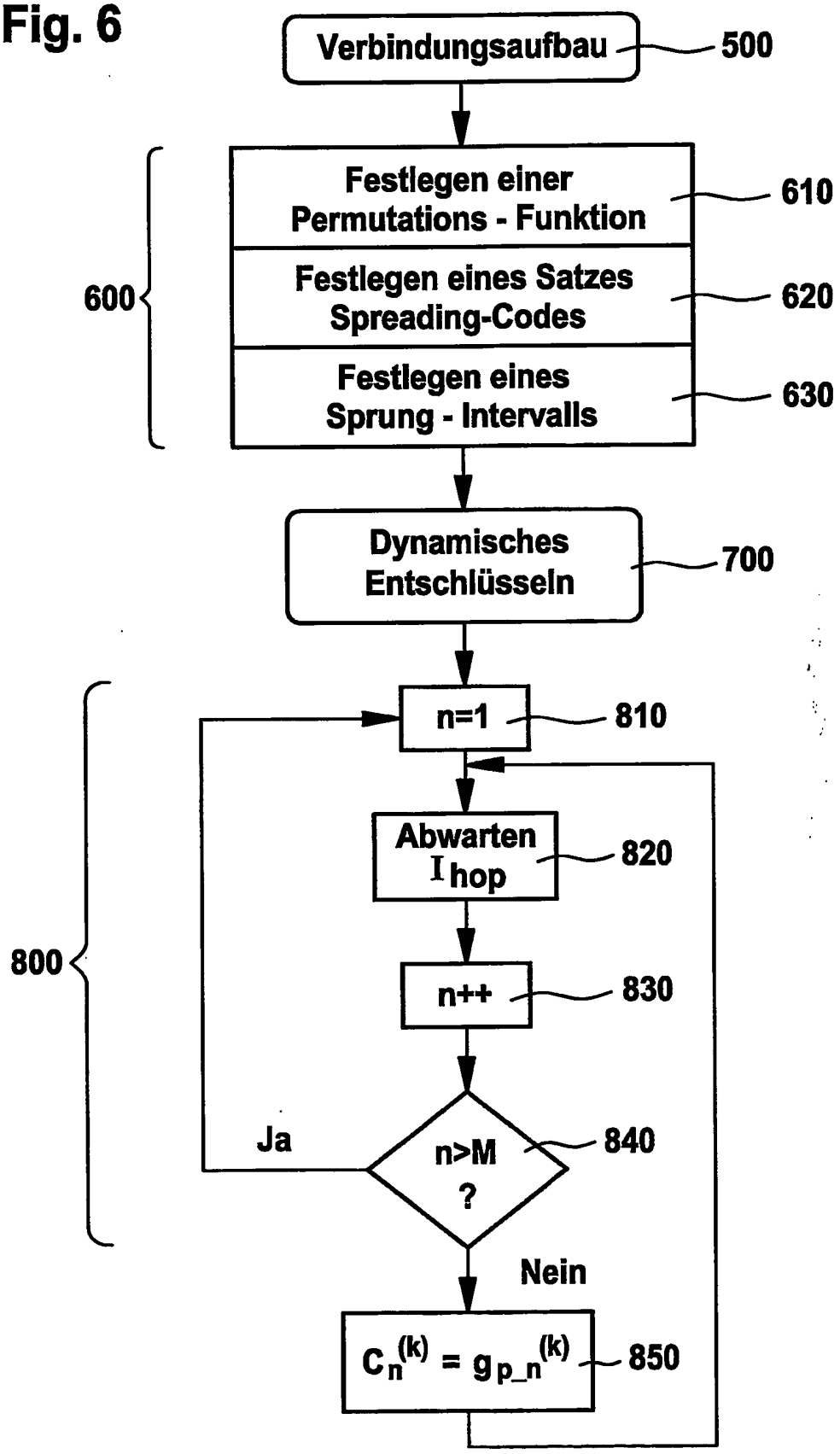
Verbindungsaufbau
500
600
Festlegen einer Permutations - Funktion
610
Festlegen eines Satzes Spreading-Codes
620
Festlegen eines Sprung - Intervalls
630
Dynamisches Entschlüsseln
700
800
n=1
810
Abwarten I hop
820
n++
830
Ja
n>M ?
840
Nein
C n (k) = g p_n (k)
850

Fig. 7

S_i =	p_1	p_2	p_3	g_{p_1}	g_{p_2}	g_{p_3}	c_j
{2, H}	2	H	-	g_2	g_H	-	g_2, g_H, g_2, g_H, g_2 ...
{5, H, 4}	5	H	4	g_5	g_H	g_4	$g_5, g_H, g_4, g_5, g_H, g_4, g_5$ ...